图书情报工作
第65卷 第8期 2021年4月

美国政府开放数据个人隐私保护政策及对我国的启示
——基于52个政策文本的内容分析

■ 储节旺 丁辉
安徽大学管理学院 合肥 230601

摘 要：[目的/意义]个人隐私保护是政府开放数据过程中的关键环节，通过对美国政府开放数据实践中的个人隐私保护政策梳理，为我国开放政府数据中的个人隐私保护提供一定的参考借鉴。[方法/过程]通过对美国政府开放数据相关政策文本的收集，运用NVivo文本分析工具，对政策文本进行内容编码分析，梳理美国政府开放数据隐私保护框架，以期获得有益的启示和借鉴作用。[结果/结论]从发挥多元主体职能作用、隐私保护评估系统构建、隐私数据利用治理、构建隐私计算模型以及法律保障5个维度来构建我国政府开放数据中的个人隐私保护体系，以最大程度发挥政府数据开放的时代价值。

关键词：政府开放数据 政策文本 个人隐私保护 美国政府开放平台
分类号：G203
DOI：10.13266/j.issn.0252－3116.2021.08.015

1 引言

随着互联网技术与经济社会发展的交汇融合，开放数据运动的广泛开展。2009年，美国奥巴马政府签署发布《开放政府指令》，将政府所掌握的信息数据资源向社会公众开放共享，由此拉开了世界政府数据开放运动的帷幕[1]。《十八届五中全会公报》提出“实施国家大数据战略”，标志着大数据战略正式上升为国家战略。我国互联网用户规模居于全球首位，拥有丰富的数据资源，政府开放数据具有较强的市场优势和发展潜力，但在开放数据中又不可避免的产生个人隐私泄露的安全问题。因此，构建政府开放数据个人隐私保护体系，对提升国家大数据治理能力、推进经济转型发展、构建服务型政府以及培育产业发展新业态具有重要的现实意义和时代价值。

在政府开放数据中的个人隐私保护方面，已取得一定的研究成果。相关研究主要是从法理、技术以及制度层面来把握，主要表现为：①关于隐私权保护的法理依据。T. Jaatinen指出，保护个人隐私数据的权利是《欧洲联盟基本权利宪章》规定的一项基本权利，个人隐私数据必须公平、合法地处理[2]；哥伦比亚大学教授A. F. Westin将隐私界定为信息自决权，即“个人、团体或机构要求确定何时、如何以及在多大程度上向他人传达有关他们的信息[3]。②从制度层面寻求突破。D. L. Baumer认为个人隐私保护制度的迟滞与不完善表现在数据跨域流动缺乏政策规制[4]；D. O. Stephens提出政府数据开放中保护个人隐私信息的原则[5]。③着眼于技术创新，加强隐私保护技术应用。C. A. Ardagna提出将XACML与PRIME相结合，可以实现基于证书管理和隐私支持功能的隐私感知访问控制解决方案[6]；胡启平提出采用xBook这种针对第三方应用程序的隐私控制平台来加强隐私保护[7]。

现有的政府开放数据隐私保护的相关研究成果对本研究具有重要的启示借鉴作用，但是研究较多的侧重于研究人员的分析归纳和理论推演，对相关隐私政策文本，运用内容分析手段进行量化分析的研究还较少。基于此，笔者运用内容分析法对美国1966年－2020年间52个关于数据安全的相关政策文本进行分析挖掘，对美国政府开放数据的个人隐私保护体系进行较为全面的分析，并针对我国政府开放数据个人隐私保护保护存在的问题提出对策建议。

作者简介：储节旺(ORCID:0000－0003－3303－4824)，教授，博士，博士生导师，E-mail:chujiewang@163.com；丁辉(ORCID:0000－0003－1950－2142)，硕士研究生。
收稿日期：2020－11－27 修回日期：2021－02－26 本文起止页码：140－150 本文责任编辑：徐健

2 研究设计

2.1 数据来源

以"Privacy protection"为搜索词，在美国"whitehouse. gov""nascio""digital. gov""congress. gov""nitrd. gov"以及"strategy. data. gov"等相关网站上，以"Information opening""Privacy data""Privacy protection""sensitive data""Intimate information"以及"High intrusion data"为关键词在政策文本类别进行检索，并按发文时间序列排序，对重复和关联性较低的文本进行剔除，共获得自1966年以来相关隐私数据保护文件共52篇(见表1)。由表1可以看出美国隐私保护相关政策文件包括法案、实施指南、备忘录、总统令等多种类型，涉及隐私权、数据管理、隐私技术、数据开放等多方面内容。因此，为了提升本研究的针对性，笔者主要从样本政策文件中提炼政府开放数据中的隐私保护的相关内容进行编码研究。

表1 美国隐私保护政策文本

时间	政策文件
1966	《信息自由法》(FOIA)[8]
1974	《隐私权法》[9]
1985	《电子交流隐私权法》
1990	《计算机比对和隐私保护法》
1996	《电子信息自由法》[10]
1998	《儿童在线隐私保护规则》
	《政府文书消除法》[11]
2000	《数据质量法》[12]
2002	《联邦信息安全管理法》
	《2002年电子政务法案隐私条款实施指南》[13]
2003	《联邦隐私法纲要》版本1.0[14]
2007	《开放政府》[15]
2009	《信息自由法案备忘录》[16]
	《透明与公开政府备忘录》[17]
	《开放政府指令》[18]
	《13526号总统令》[19]
2010	《13556号总统令》[20]
	《OMB M-10-22》[21]
	《OMB M-10-23》[22]
2011	《国家行动计划1》
2012	《消费者数据隐私保护法案》[23]
	《建设21世纪数字政府备忘录》
2013	《13642总统令》[24]
	《国家行动计划2》[25]
	《政府信息的默认形式就是开放和机器可读》[26]
	《开放数据项目》[27]
	《开放数据政策:将信息作为资产管理》[28]
2014	《开放数据计划》[29]
	《大数据:抓住机遇,保持价值》[30]
2015	《电子通信隐私法修正案(2015)》[31]
	《OMB M-15-13》[32]
2016	《开放政府数据法案》[33]
	《OMB Circular A-130》[34]
	《国家隐私研究战略》[35]
	《欧盟-美国隐私保护指南》[36]
2017	《约束性操作指令》[37]
	《OMB M-17-06》[38]
	《使用密码术的隐私保护协作》[39]
	《SP 800-53的第五修订草案》[40]
2019	《NASCIO隐私保护指导原则》[41]
	《S. 783-2019年儿童上网清洁法案》[42]
	《S. 189-2019媒体隐私保护和消费者权益法》[43]
	《S. 583-数据隐私法》[44]
	《S. 1842-保护个人健康数据法》[45]
	《S. 1214-隐私权法案》[46]
	《S. 2961-2019年数据保护法案》[47]
2020	《约束性操作指令20-01》[48]
	《S. 4626-安全数据法》[49]
	《S. 3300-2020年数据保护法》[50]
	《2020年行动计划》[51]
	《HR5678-隐私权办公室增强法》[52]
	2020年《应用程序隐私,保护和安全法》[53]

2.2 研究方法

基于研究的现实需要，笔者主要采用内容分析法对政策文本进行分析。主要涉及以下3个步骤:①通过对关键词"信息公开""隐私数据"以及"隐私保护"等搜索，将收集的52份政策文本进行逐一分析与初步归类;②运用Nvivo12 Plus软件对收集的样本文字内容进行词频分析(word frequency analysis)、核心关键词句编码(coding)以及生成可视化(visualization)图表;③在Nvivo计量统计与分析的基础上，对美国政府开放数据的隐私保护框架进行系统梳理，进而为我国政府开放数据个人隐私保护提供借鉴作用。

3 美国政府开放数据中隐私保护政策文本的内容分析

3.1 美国隐私保护政策文本的基本概况

通过对美国相关网站获取的52份政策文本，可以看出美国关于个人隐私保护的实践起源较早，以20世纪60年代《信息自由法》为标志，拉开了公民获取信息

权利以及信息隐私保护的序幕。之后,美国个人隐私保护的政策文件相继出台,涉及内容范围不断扩大、隐私保护程序规范性不断提升、隐私保护框架趋于完善。笔者从政策出台时间、政策发布主题对美国政府开放数据隐私保护的基本概况进行梳理。

3.1.1　政策出台时间

根据前文政策文本的整理可以看出早在 2000 年之前,美国就已经逐步开展隐私政策文件的制定工作。步入 21 世纪,自奥巴马政府推进政府开放数据的实践,美国隐私政策文件骤增,2010 年之后出台的文件数量总和占据整个政策文件数量的 69%。因此可以看出:①随着政府开放数据实践的深入发展,隐私数据保护逐渐成为当前政府数据开放过程中所面临的严峻问题;②美国政府开放数据的政策体系框架日趋成熟,这对我国的隐私政策的制定具有重要的启示借鉴作用。

3.1.2　政策发布主题

通过对所获取的政策文本的主题提炼,现有的美国政府开放数据中的个人隐私政策文本主题呈现多元分布,主要有隐私权、儿童隐私保护、电子信息隐私、政府信息安全、数据利用、隐私保护指令、行动计划以及隐私法案 8 大类(见图 1)。其中最多的是隐私法案和隐私保护指令政策主体样本。表明在美国现有的隐私保护框架体系下,一方面通过宏观立法的形式,给予公民隐私保护以法律效力;另一方面,以隐私保护指令的形式,细化各部门隐私保护的途径与程序,确保隐私保护有例可循,提高了隐私保护的可行性。

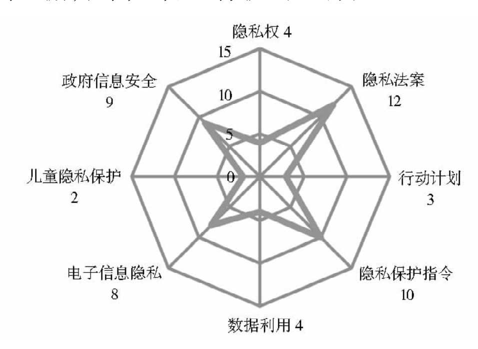


图 1　政策主题

同时对高频关键词云统计显示(见图 2),可以看出美国政府开发数据隐私保护的政策文本的主要内容侧重于 4 个着力点:①推进隐私保护的立法工作;②加强隐私信息数据生命周期的利用治理(收集、利用、控制、评估);③落实隐私保护的主体责任(OMB、第三方网站、NASCIO 等);④完善隐私保护的程序。四大维度表明,美国政府数据开放隐私保护框架既具有宏观层面的指导意义,又具有微观层面的可操作性。

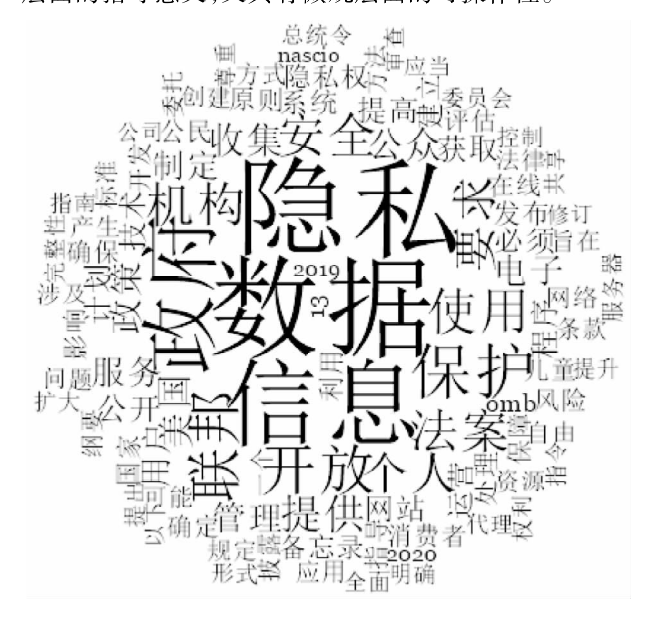


图 2　高频关键词云图

3.2　美国政府数据开放隐私安全政策内容的编码分析

在内容分析法中,"需要确定分析单元,即挖掘研究应考察的各项因素,这些因素应与分析目的有一种必然的联系,且便于抽取操作"[54]。笔者将收集的 52 份样本政策文件中关于数据隐私保护的相关内容作为基本分析单元。在政策节点类型划分方面,由于选取的是美国政府出台的相关政策文件,主要以公共政策为主,因此借鉴公共管理领域的常用政策划分方法,将美国隐私保护政策分为程序性政策与实质性政策两类。同时为保证参考节点的可靠性与一致性,两位笔者分别独立对政策文本进行编码,并对编码结果的一致率进行了计算,计算结果基本符合效度信度检验标准。据此,从程序性政策供给与实质性政策供给两个层面,制定了 9 个分析节点的编码规则(见图 3)。依

名称	文件	参考点
程序性政策	0	0
保护程序	13	17
评估审查	12	14
隐私机构	17	26
隐私框架	17	22
实质性政策	0	0
公民隐私权利	14	20
数据保护类型	20	26
数据利用	24	29
隐私保护标准	13	17
隐私保护技术	13	22

图 3　主要节点编码分析

据编码规则,借助 Nvivo 12 Plus 中的关键词搜索功能,从 52 份政策文本中挖掘出了 79 个程序性政策层面的

参考点、114 个实质性政策层面的参考点。

3.2.1 隐私保护程序性政策编码分析

所谓程序性政策是指虽然不产生实质性后果,但通过明确规定政府的活动程序,来规范和约束政府的行为,约束公共权力的政策。根据既有文献研究成果和所获取的文本资料,将隐私保护程序、评估审查、隐私机构以及隐私框架作为程序性政策的研究维度。表 2 为美国政府开放数据隐私保护程序性政策的单元编码。

表 2 程序性政策层面节点编码

主体维度	维度解释	主要标志词句
保护程序	实施隐私保护的相关程序	确定管理和监督国土安全部记录,管理政策和程序的方法;通过程序和信息系统处理 PII(Personally Identifiable Information);建立了新的程序,并提供了最新的指导和机构使用网络测量和定制技术的要求等
评估审查	建立隐私数据的评估审查机制	为了帮助各州确定和评估可能对其信息系统和政策造成隐私影响的联邦法律,NASCIO 开发了 1.0 版《联邦隐私法纲要》;应监测任何更改第三方的隐私政策并定期重新评估风险;各部门都必须建立相应的数据审查复核机制等
隐私机构	隐私保护的管理体系中设置的多元主体	PRA(Paperwork Reduction Act)通常要求联邦机构:发布联邦公报通知,以征询公众对拟议收集的意见;OPCL(Office of Privacy and Civil Liberties)编写《隐私法》的禁止披露;OMB(Office of Management and Budget)的主任必须为联邦各个部门数据发布工作制定细则
隐私框架	隐私数据保护政策的基本框架	为开放政府创造有利的政策框架;规定了联邦政府信息资源公开和获取的基本框架和程序等

从表 2 中的编码分析可以看出,美国在政策指导层面既注重出台相关法律政策、隐私保护程序和基本框架为隐私保护提供根本遵循,又重视发挥多元主体的能动作用,落实主体责任。通过对相关文本的内容以及编码分析,可以将美国程序性隐私保护框架归纳为两类:

(1)法律体系:夯实隐私保护的基石。以 1967 年美国的《信息自由法》为开端,美国隐私权法案不断完善丰富。以 2009 年美国建立第一个政府开放数据平台 www.data.gov 为契机,美国政府开放数据中的隐私保护法案相继出台。以奥巴马政府颁布的《信息自由法备忘录》[55]为行动指南,以《隐私政策》[56]《开放数据政策》《开放政府数据法》等法案为遵循,主要有两方面的内容:①对收集数据的审查:联邦政府机构需对收集的数据进行日常审查,对隐私泄露、安全风险、法律责任、知识产权限制等因素进行考虑,以确定是否公开数据;②增强数据的透明度:所收集的个人数据及其必要性、使用目的、预计删除日期、是否与第三方共享以及共享的目的,要向公民进行说明,以增强公民隐私保护意识。隐私法案的完善是当前美国政府开放数据实践取得良好效果的重要保障因素。

(2)管理体系:强化隐私保护的责任。组织机构的设立是履行隐私保护责任的必要措施。如表 3 所示,美国在隐私保护的管理体系中设置多元主体,分担不同职能、承担不同责任、管理数据周期不同阶段,以强化隐私保护责任,实现政府开放数据的利益最大化。管理和预算办公室(OMB)是总统办公厅内的一个机构,致力于确保拟议的立法与行政政策相一致。2002 年《电子政务法》的规定使得 OMB 成为保护美国公民隐私的最高权力机构,为隐私保护提供必要的指导和监督[57]。信息政策办公室(Office of Information Policy,OIP)任务是鼓励和监督机构遵守《信息自由法》,就《信息自由法》管理的各个方面制定政府的政策指导,同时向机构人员提供法律咨询和培训[58]。首席信息官委员会(CIO)是改进联邦信息资源设计、获取、开发、现代化、使用、共享和性能相关的机构间主要论坛,为规范实施数字隐私控制和教育机构隐私制定实施指南[59]。联邦隐私委员会(Federal Privacy Commission,FPC)通过确定和分享经验教训和最佳实践,改善对机构隐私计划的管理;促进机构隐私专业人员之间的合作,以减少不必要的重复工作,并确保在政府范围内有效、高效和一致地实施隐私政策[60]。国家技术情报服务处(National Technical Information Service,NTIS)通过与私营部门的合作,向联邦机构提供创新的数据服务,以推进联邦数据优先事项,促进经济增长,所收集的信息将在 NTIS 中采取必要的保存措施,以保护数据隐私[61]。美国总务管理局(General Services Administration,GSA)按照隐私法案的规定,对于个人身份信息(PII)进行定期审查,以确保个人数据的完整性、正确性、必要性,同时使用隐私影响评估(Privacy Impact Assessment,PIA)作为一个关键工具,以确保隐私问题和保护能够在包含任何 PII 的信息技术系统中得到解决[62]。

表 3 美国隐私保护机构及其职能

管理体系	组织机构	义务职能
领导机构	管理和预算办公室	对隐私保护的指导和监督
执行机构	信息政策办公室	提供隐私政策指导和法律培训
	首席信息官委员会	制定隐私政策实施指南
	联邦隐私委员会	隐私计划管理和人员合作
	国家信息技术局	信息保存过程中的隐私保护
评估机构	美国总务管理局	对隐私影响进行评估

3.2.2 隐私保护实质性政策编码分析

所谓实质性政策是指：具有到位的物质资源投入，有明确的执行授权，对政策调适对象或是有明确的切实利益提供，或是有明确具体的行为规范，同时有严密的组织程序辅助执行的政策。根据实质性政策的定义以及所获得的文本内容的实际，笔者将实质性政策细化为公民隐私权利、数据保护类型、数据利用、隐私保护标准以及隐私保护技术5个研究维度，如表4所示：

表4 实质性政策层面节点编码

主体维度	维度解释	主要标志词句
公民隐私权利	公民隐私权的维护	司法部的隐私和公民自由办公室编写《隐私权法案》；政府不得在未被允许的情况下截取、监听私人电子通讯，电子交流隐私权得到保障；适用于隐私保护的公司的义务包含在"隐私权原则"中等
数据保护类型	细化数据类型，制定不同的隐私数据保护政策	切实保护了个人隐私权以及个人信息在互联网中的使用；重点明确将提高电子信息通信中对于隐私权的保护；该法案要求联邦贸易委员会(Federal Trade Commission，FTC)制定有关收集个人信息的规则，以提高消费者的隐私；从儿童或有关儿童那里收集的个人信息对于响应司法程序或向执法机构提供信息是必需的等
数据利用	数据获取、利用过程中的隐私保护	核心是整合公众力量、加强获取、提升管理，给公众更多的话语权；任何此类技术的使用必须尊重隐私、公开和透明；该指南指导各机构在使用信息技术收集新信息时，如何在其机构内处理有关个人的信息等
隐私保护标准	数据开放、利用的标准规范	为敏感信息建立标准，减少对公众的过度隐瞒；要求政府机构构建一个线上资源中心，提供给公众，并提出要采用新的数据标准提高可读性；规范数据格式，制定开放数据的统一标准，提升数据的易用性等
隐私保护技术	运用在隐私数据保护领域的相关计算机技术	通过采用隐私保护技术(如安全多方计算)，改善政府使用和保护数据的方式；护数据完整性：将最先进的数据安全作为信息技术安全实践的一部分，针对每一个更新、构建或替换的系统，以解决当前和新出现的威胁；促进创新并利用新技术来维护保护等

表4列出了美国政府开放数据实质性政策层面的内容编码，通过编码分析可以看出程序性政策为美国隐私数据保护提供了顶层设计，而实质性政策则是将程序性政策的要求由顶层设计向问计于民的系统转化。通过对隐私数据保护的实质性政策的节点编码以及政策文本的内容分析，可以将美国政府数据开放隐私政策体系归纳为3类：

(1)策略体系：提升隐私保护的核心。数据的使用正在改变世界。联邦政府提供、维护和使用数据的方式在社会上有着独特的地位，保持对联邦数据的信任是民主进程的关键。为了满足不断变化的数据角色和民主需求，联邦政府制定了一个协调和综合的数据战略，使数据能够更好地在任务中传递、服务于公众和管理资源，同时尊重隐私和保密性[63]。

建立数据PII清单：为了正确评估和减轻其数据服务或程序的隐私风险，机构必须首先知道可以收集、维护、使用或披露哪些PII(见表5)。任何PII清单或目录都不可能足够或完整的理解哪些个人信息应被视为"可识别"。在通常的认知中，PII仅包括可用于直接识别或联系个人的数据(如姓名)或特别敏感的个人数据(如银行账号)。OMB和NIST对PII的定义更为宽泛，定义也是动态的。通过多种碎片化数据的整合分析(如年龄、身高)仍然可以构成PII。换言之，如果数据被链接或可以链接到特定的个人("可链接")，则可能是PII。

个人的通知和补救：根据《隐私法》的要求，各组

表5 PII清单[64]

数据类型		影响(低、中、高)
个人识别码	姓名	
	社会保障号码	
	驾驶证号码	
	信用卡号码	
	其他金融账号(银行等)	
	护照号码	
	其他政府ID或唯一标识符	
联系方式	电子邮件地址	
	电话号码	
	邮政地址	
其他个人资料	用户名、头像等。	
	娘家姓	
	出生日期	
	性	
	年龄	
	其他物理描述(眼睛/头发颜色、身高等)	
	婚姻状况/子女/亲属	
	性取向	
	种族	
	宗教	
	教育类	
	就业	
	公民身份	
	健康、保险、治疗或医疗信息	
	犯罪史	
	其他PII(例如，在用户填写的非结构化数据字段中)	

（续表5）

数据类型		影响（低、中、高）
生物识别数据	签名	
	指纹、手印	
	照片、扫描（视网膜、面部）	
	语音	
	身体动作（例如手指滑动、击键）	
	DNA标记	
设备相关数据	用户名	
	密码	
	唯一设备标识符	
	位置/GPS数据	
	摄像机控制（照片、视频、视频会议）	
	麦克风控制	
	其他硬件/软件控制	
	照片数据	
	音频/声音数据	
	其他设备传感器控制或数据	
	开/关状态和控制	
	信号塔记录（如日志、用户位置、时间、日期）	
	应用程序收集的数据（逐项列出）	
	联系人列表和目录	
	生物测定数据或相关数据（见上文）	
	SD卡或其他存储数据	
	网络状态	
	网络通信数据	
	设备设置或首选项（如安全、共享、状态等）	
网站相关数据	日志数据（如IP地址、时间、日期、浏览器类型）	
	跟踪数据（例如，单会话或多会话cookies、信标）	
	表单数据	

织必须制定并在《联邦公报》中公布补救政策和程序，对不准确、不相关、不及时或不完整的数据的修正或更正[65]。涉及以下内容：①通知：通知应告知个人收集的信息、收集的目的、如何使用信息、向其披露和共享信息的人、个人的权利、以及可用的补救计划类型、保留信息的时间以及未能提供所要求的信息后果；②管理隐私投诉和补救：组织还应制定管理隐私投诉或查询的政策和程序确保所有投诉都得到记录、跟踪和处理；③文件：政策和程序文件提供详细的隐私投诉解决程序：补救者权利、人员补救政策程序培训、补救和投诉处理过程的说明、建立服务标准以及程序的公开透明；④报告：组织应跟踪内部和外部报告的隐私投诉以用于识别组织中可能需要进一步处理的领域。通知和补救措施对于实现信息公开透明度和个人参与至关重要——这是两项基本的公平信息实践原则。

（2）技术体系：织密隐私数据的防护网。网络和信息技术研究与发展（Network and Information Technology R&D，NITRD）计划是美国联邦政府计算机、网络和软件先进信息技术研发（R&D）获得资助资金的主要来源方式。NITRD是最古老、规模最大的正式联邦计划之一，该计划协调多个机构的活动，以解决多学科、多技术和多部门的研发需求[66]。在政府开放数据的过程中，NITRD计划所带来的技术支持是维护隐私数据的强力支撑。

隐私保护数据匹配：记录匹配通常在不同的数据源之间执行，目的是识别这些数据源之间共享的公共信息。然而，来自不同数据源的匹配记录通常与有关数据的隐私要求形成矛盾。为了缓解安全性与隐私性之间的矛盾，美国联邦政府在数据收集过程中运用安全多方计算（Secure Multiparty Computing，SMC）和数据净化方法（如差分隐私和k－匿名）技术相结合，以实现对大型数据集中的数据加密，减少数据匹配中的隐私泄露风险。

隐私特征脱敏处理：在用户必须与许多不同的服务提供商进行交互的分布式环境中，生物特征模板的敏感信息保护变得更加复杂。为此联邦政府组织采用感知哈希技术、分类技术和零知识证明知识（zero-knowledge proof of knowledge，ZKPK）协议[67]。在这种方法下，对用户的生物特征模板进行处理以从中提取一串比特，通过分类和其他某种转换对其进行进一步处理，将所得的位串与随机数一起用于生成密码承诺。此承诺代表一个识别令牌，不会透露任何有关原始输入的生物识别信息。将承诺用于ZKPK协议以对用户进行身份验证。

（3）评估体系：增强隐私保护的效果。美国具备完善的隐私评估领导机构（见图4）。国土安全部隐私办公室（Department of Homeland Security，DHS）对技术、规则制定、计划和活动进行数字隐私影响评估（PIA），无论其数据分类类型如何，以确保将隐私考虑和保护纳入部门的所有活动中[68]。PIA是对个人身份信息如何收集、使用、传播和维护的分析。PIA的目的是证明程序管理员和系统所有者在系统或程序的整个开发生命周期中有意识地纳入了隐私保护[69]。PIA分析如何处理信息，以确保此类处理符合有关隐私的适用法律、法规和政策要求，为了降低潜在的隐私风险，确定收集、维护和传播此类信息的风险和影响，并检查和评估处理信息的保护和替代过程，必须记录PIA过程。

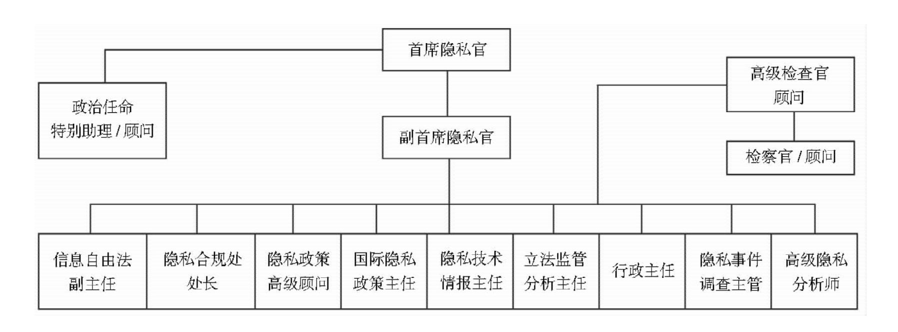


图4 美国隐私评估领导机构

通过对52份政策文本的内容编码分析,可以看出在美国政府开放数据的过程中,个人隐私保护政策的制定与实施一直是其关注的关键环节。其对个人隐私数据的保护涉及法律体系、管理体系、策略体系、技术体系以及评估体系5大维度,贯穿政府开放数据的整个周期,这为美国政府开放数据价值的创造提供了政策层面的保障。同时,也为我国开放型政府的构建以及公民隐私权利的保障提供了双重借鉴作用。

4 美国政府开放数据个人隐私保护体系对我国的启示

借鉴美国政府开放数据中的个人隐私政策体系和措施,完善我国政府开放数据中的个人隐私保护可从采取以下方面的对策:

4.1 发挥多元主体的职能作用

美国针对数据开放中产生的隐私泄露问题,建立了CIO制度以及DHS机构。通过设立首席信息官职来专职于政府数据开放工作。同时,美国管理与预算办公室(OMB)以及美国总务管理局(GSA)都承担了对隐私过程的审查和部分监管职能。我国现阶段已建立中共中央网络安全和信息化委员会办公室以及国家互联网信息办公室等相关机构。因此,在政府开放数据过程中要发挥相关机构的职能来承担政府开放数据中的隐私保护和网络安全的职责:①出台个人隐私数据实施标准化建议:在个人隐私数据获取前,要对数据类型进行识别,制定出个人隐私数据的项目清单;公民在政府网站填写提交自身个人数据信息,要有相应的隐私声明,告知公民收集的目的、权限等。②设立个人隐私数据利用的原则:按照透明度、个人参与、完整性、一致性、最小化、使用告知、使用限制以及允许修改等原则来收集利用个人数据。③审查监督数据开放过程:隐私机构的第三项职责就是对政府开放数据的整个生命周期进行严格的审查和监督。④加强员工的培训:打造一支专业化的信息安全和隐私保护团队,作为能动的主体,对相关人员的培训是至关重要的。要加强员工隐私意识和职业操守的培训。⑤细化落实主体责任:隐私机构要严格遵循相关法律法规,对个人隐私泄露过程中的相关主体的责任要落实到位,防止推诿扯皮现象的发生,对违反法律法规的行为进行处罚,以构建公开透明的隐私工作团队。

4.2 构建隐私评估系统

个人隐私数据影响评估是指针对个人隐私数据的收集利用,检验其合法合规程度,判断其对个人隐私数据主体合法权益可能造成损害的各种风险,以及评估用于保护个人信息主体的各项措施有效性的过程。2003年,美国发布《隐私影响评估指南》(Privacy Impact Assessment Guide,PIA),该指南提供了一个框架,用于进行隐私影响评估,即用可识别的方式对收集、储存、保护、分享和管理的信息进行分析,以评估如何在信息系统中管理个人身份信息[70]。

这对我国政府开放数据中隐私影响评估系统的构建有着重要的启示借鉴作用。①组建隐私评估主体:由政府牵头,由不同领域的专家学者组建一个隐私评估主体机构,对个人隐私数据的合规性和开放过程的安全性进行评估。②健全隐私评估措施:可以借鉴美国PII清单中对个人隐私数据特征的分类,按照个人隐私数据敏感程度来实施不同的评估标准。③完善隐私评估流程:如图5所示,对政府数据平台的数据集进行预评估以确定进行隐私风险影响评估的重要性,其次进行评估准备,从收集、处理、使用、分享、删除全流程对数据进行记录,并分析不同流程对个人权益和信息安全带来的影响以确定其风险,最后做出评估报告。

4.3 加强数据利用治理

4.3.1 构建数据清单

对那些“可识别”的数据元素(如电话号码、身份证号码、照片)列入数据清单并对数据元素对个人隐私泄露的高低进行排列。在政府收集个人数据时,以数

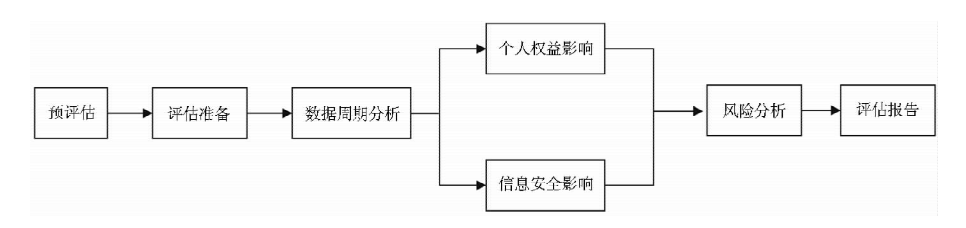


图5 隐私评估流程

据清单为参照,尤其是对个人隐私泄露有重大影响的数据元素的采集,要按照数据收集最小化的原则,只收集与政府工作有必然联系的个人数据,同时只保留必要的个人信息,以实现数据生命周期的最小化。

4.3.2 提升隐私保护技术

技术的进步对于提升政府数据开放水平和个人隐私数据的保护具有重要作用,要注重利用技术手段加强对个人隐私数据的保护。①数据加密。政府数据库涵盖了大量的个人信息,对敏感数据进行加密是保护个人隐私数据的重要途径。对系统中数据进行加利用加密函数或者密钥实现政府部门数据库管理系统平台对接外界硬件时密码运算,利用数据加密计算判断政府部门的数据库系统平台是否允许数据访问传输,并将数据库的安全隐患及时反馈给网络数据的操作端口,避免数据库信息、网络密钥的恶意盗取与篡改,可以有效保护政府的重要信息[71]。②建立数据传输通道保护系统。政府数据开放平台与用户间的数据传输通信过程如果不是安全信道,则极易数据被第三方截取、篡改、污染等,难以保障数据传输的真实性、机密性和完整性[72]。通过对通信双方(服务端、客户端)进行IP地址、端口、及一些传输内容的控制,来优化数据传输环境,增强数据传输能力,保证数据传输通道的安全性、高效性。③审计日志。审计是将用户操作数据库的所有记录存储在审计日志(audit log)中,它对将来出现问题时可以方便调查和分析有重要的作用。对于系统出现问题,可以很快地找出非法存取数据的时间、内容以及相关的人。从软件工程的角度上看,目前通过存取控制、数据加密的方式对数据进行保护是不够的。因此,作为重要的补充手段,审计方式是安全的数据库系统不可缺少的一部分,也是数据库系统的最后一道重要的安全防线。

4.4 构建基于政府开放数据周期的隐私计算模型

信息技术的广泛应用为政府数据的收集、储存、保护、发布、销毁等带来极大便利,同时也让个人隐私数据泄露的风险贯穿于整个政府开放数据的生命周期之中。借鉴美国在隐私保护阶段采用的差分隐私和k－匿名技术以及在隐私处理阶段采用的数据脱敏技术的做法,我国可以构建基于数据开放周期的隐私计算模型。隐私计算是面向隐私信息全生命周期保护的可计算模型与公理化系统[73]。①隐私信息收集:在政府收集的个人信息中对包含个人隐私的敏感数据进行特殊化处理(标记或编码),进而建立隐私元数据集合。②隐私数据储存:根据收集阶段建立的隐私变量集合采用重复数据删除等技术来降低同质数据的重复率,减少隐私数据存量。③隐私数据保护:采用SMC、密码术以及差分隐私等技术来满足对储存阶段保留的隐私数据源的保护需求。④隐私数据发布;在政府数据开放阶段,根据发布信息的属性、场合、数据敏感程度采用感知哈希技术、数据脱敏处理以及ZKPK协议等相应的技术来公开数据。⑤隐私数据销毁:在数据开放周期结束后,对于不再需要开放的包含隐私信息的数据可采用确定性删除技术进行彻底销毁。在信息化时代,构建基于政府开放数据周期的隐私计算模型,为个人隐私保护提供一套系统化、理论化的计算模型是现阶段我国开放型政府建设的重要环节。

4.5 健全隐私保护法律体系

虽然近几年我国针对互联网环境下的个人信息保护制定了《关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律文件,然而缺乏专门的个人信息保护基本法。我国现阶段的政府开放数据方面的法律内容更多的是与信息公开相关而并没有深入到数据获取利益的层面。因此,现阶段我国应该制定一部《政府数据开放法》。首先,在法律中对我国政府数据开放的程序、内容进行法律规定,规范政府数据开放的过程,减少数据开放的随意性,平衡好“开放政府”与“个人隐私”之间的矛盾;其次,《政府开放数据法》要对“个人隐私”的概念进行法律界定,以对政府开放数据中侵犯“个人隐私”的行为进行判定,降低个人隐私泄露的风险;最后,要完善公民“个人隐私”的审查和补救制度,对侵犯公民“个人隐私”的行为能够进行回溯分析,能够准确的发现隐私泄露的环节,同时要进行追踪处理,对“个人隐私”的补救要落实到

位,以保障公民的合法权利。通过制定《政府数据保护法》的方式,减少政府开放数据中的个人隐私泄露的风险,提高政府开放数据的时代价值,为我国开放政府、服务型政府的构建保驾护航。

5 结语

政府开放数据是大数据时代,激发数据活力,创造巨大社会价值的重要实践,同时也是推进透明型、服务型政府以及我国国家治理体系和治理能力现代化的重要举措。政府数据开放过程中必然会产生个人隐私泄露的问题。笔者通过对美国联邦政府开放数据中的相关实践和措施进行梳理,为我国政府开放数据中的个人隐私保护提供一些借鉴和思考。我国应从主管机构、隐私评估、数据治理、隐私模型以及法律保障5个维度着手,从机构部门的设置、人员的培训、数据开放的审查监督、隐私影响的评估、技术手段的利用、法律的制定等方面,细化个人隐私保护的对策,构建较为完善的个人隐私保护体系,以保障政府开放数据中公民的合法权利,同时为政府开放数据所带来的价值更好的服务于人民夯实基础。

参考文献:

[1] Office of management and budget(OMB). Open government directive,M – 10 – 06[EB/OL].[2020 – 07 – 20]. http://www.whitehouse.gov/omb/assets/memoranda-2010/m1006.pdf.
[2] JAATINEN T. The relationship between open data initiatives,privacy,and government transp-arency:a love triangle[J]. International data privacy law,2016,6(1):28 – 38.
[3] WESTIN F. Science,privacy,and freedom: issues and proposals for the 1970s. Part 1 the current impact of surveillance on privacy[J]. Columbia law review,1966,66(6):1003 – 1050.
[4] BAUMER D L, EARP J B,POINDEXTER J C. Internet privacy law:a comparison between the United States and the European Union[J]. Computers & security,2011,23(5):400 – 412.
[5] STEPHENS D. Protecting personal privacy in the global business environment: in the electronic world,protecting personally identifiable information is a critical challenge for all companies and governments[J]. Information management journal,2007,41(3): 56 – 59.
[6] ARDAGNA C A,DCD VIMERCATI S,PARABOSCHI S,et al. An xacml-based privacy-centered access control system[C]//Proceedings of the first ACM workshop on Information security governance. New York:ACM,2009:49 – 58.
[7] 胡启平,陈震. 试析社交网络环境中个人隐私保护[J]. 信息网络安全,2010(8):43 – 44.
[8] Freedom of information act[EB/OL].[2020 – 08 – 01]. http://www.whitehouse.gov/the_press_office/Freedom of Information Act/.
[9] Privacy protection act[EB/OL].[2020 – 08 – 02]. https://www.justice.gov/opcl/overview-Privacy-act-1974-2015-edition.
[10] 谢恩平. 美国的《信息自由法》与媒体[D]. 北京:中央民族大学,2006.
[11] Digital government[EB/OL].[2020 – 08 – 03]. https://digital.gov/resources/paperwork-reduction-act-fast-track-process/.
[12] Data quality act of 2000[EB/OL].[2020 – 08 – 13]. http://www.whitehouse.gov/sites/default/files/omb/fedreg/reproducible2.pdf.
[13] E-government bill[EB/OL].[2020 – 08 – 04]. https://obamawhitehouse.archives.gov/omb/mem-oranda_m03-22/.
[14] Federal privacy act[EB/OL].[2020 – 08 – 05]. https://www.nascio.org/resource-center/resou-rces/federal-privacy-law-compendium-version-1-0/.
[15] Open government act of 2007[EB/OL].[2020 – 08 – 06]. https://www.govtrack.us/congress/bills/110/s2488/text.
[16] Freedom of information act (2009)[EB/OL].[2020 – 08 – 07]. http://www.whitehouse.gov/the_press_office/Freedom_of_Information_Act.
[17] Transparency and open government[EB/OL].[2020 – 08 – 09]. http://www.whitehouse.gov/the_press_office/Transparency and Open Government/.
[18] Open government directive[EB/OL].[2020 – 08 – 10]. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.
[19] Executive order 13526 – classified national security information[EB/OL].[2020 – 08 – 11]. https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.
[20] Executive order 13556 – classified national security information[EB/OL].[2020 – 08 – 11]. https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.
[21] Office of management and budget[EB/OL].[2020 – 08 – 14]. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.
[22] Office of management and budget[EB/OL].[2020 – 08 – 14]. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.
[23] Consumer data privacy in a networked world[EB/OL].[2020 – 08 – 16]. http://www.white-house.gov/sites/default/files/privacy-final.pdf.
[24] Executive order 13642-- making open and machine readable the new default for government information[EB/OL].[2020 – 08 – 17]. https://www.Whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government.
[25] Second national action plan[EB/OL].[2020 – 08 – 18]. http://

www. whitehouse. gov /sites/default/files/docs/us_national_action_plan_6p. pdf.
[26] Executive order-making open and machine readable the new default for government information[EB/OL]. [2020-08-20]. http://www. whitehouse. gov/the -press-office/2013/05/09/executive-order- making-open -and -machine-readable - new- default-government -.
[27] Common core metadata schema v1.0[EB/OL]. [2020-08-22]. https://project-open-data. cio. gov/schema/.
[28] RASHM K, YUKIKA A. Liberating data for public value: The case of Data. gov. [J]. International journal of information management, 2016, 36, (4): 668-672.
[29] US-open-data-action-plan [EB/OL]. [2020-09-03]. https://www. whitehouse. gov /sites/default/files/microsites/ostp/us_open_data_action_plan. pdf.
[30] Big data, open data & the federal agencies - digital. gov[EB/OL]. [2020-09-05]. https://digital. gov/2014/07/01/big-data-open-data-the-federal-agencies/.
[31] The electronic communications privacy act amendments act of 2015 [EB/OL]. [2020-09-11]. https://www. govtrack. us/congress/bills/114/hr283/text.
[32] Office of management and budget[EB/OL]. [2020-09-14]. https://obamawhitehouse. archives. gov/sites/default/files/omb/memoranda/2015/m-15-13. pdf.
[33] Open, public, electronic, and necessary government data act or the open government data act[EB/OL]. [2020-09-17]. https://www. congress. gov/bill/114th-congress/senate-bill/2852.
[34] Office of management and budget[EB/OL]. [2020-09-18]. https://www. whitehouse. gov/sites/whitehouse. gov/files/omb/circulars/A130/a130revised. pdf.
[35] National privacy strategy[EB/OL]. [2020-09-21]. https://www. nitrd. gov/PUBS/National Priv-acy Research Strategy. pdf.
[36] Privacy guide[EB/OL]. [2020-09-24]. https://ec. europa. eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en. pd_. pdf.
[37] Cyber. dhs. gov -binding operational directive 18-01[EB/OL]. [2020-09-30]. https://cyber. dhsgov/bod/18-01/.
[38] Office of management and budget[EB/OL]. [2020-10-03]. https://www. whitehouse. gov/sites/whitehouse. gov/files/omb/memoranda/2017/m-17-06. pdf.
[39] Privacy protection technology[EB/OL]. [2020-10-05]. https://digital. gov/resources/privacy-preserving-collaboration-using-cryptography/.
[40] Digital. government[EB/OL]. [2020-10-11]. https://digital. gov/2017/08/22/nist-crafts-next-generation-safeguards-for-information-systems-and-the-internet-of-things/.
[41] Privacy guidelines[EB/OL]. [2020-10-13]. https://www. nascio. org/privacy-policy/.
[42] Children's internet bill[EB/OL]. [2020-10-17]. https://www. congress. gov/bill/116th-congress/senate-bill/783? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=3.
[43] Social media privacy protection and consumer rights law [EB/OL]. [2020-10-20]. https://www. congress. gov/bill/116th-congress/senate-bill/189? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=7.
[44] Data privacy law [EB/OL]. [2020-10-24]. https://www. congress. gov/bill/116th-congress/senate-bill/583? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=17.
[45] Personal health data protection act [EB/OL]. [2020-10-28]. https://www. congress. gov/bill/116th-congress/senate-bill/1842? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=50.
[46] Privacy act [EB/OL]. [2020-11-02]. https://www. congress. gov/bill/116th-congress/senate-bill/1214? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=48.
[47] Data protection act[EB/OL]. [2020-11-07]. https://www. congress. gov/bill/116th-congress/senate-bill/2961? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=57.
[48] Cyber. dhs. gov - binding operational directive20-01[EB/OL]. [2020-11-10]. https://cyber. dhsgov/bod/20-01/.
[49] Data security law[EB/OL]. [2020-11-13]. https://www. congress. gov/bill/116th-congress/senate-bill/4626? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=56.
[50] Data protection act 2020[EB/OL]. [2020-11-13]. https://www. congress. gov/bill/116th-congr-ess/senate-bill/3300? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=32.
[51] 2020 action plan[EB/OL]. [2020-11-14]. https://strategy. data. gov/practices/.
[52] Privacy office enhancement Act[EB/OL]. [2020-11-15]. https://www. congress. gov/bill/116th-congress/house-bill/5678? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=6.
[53] Application privacy and security protection law[EB/OL]. [2020-11-16]. https://www. congress. gov/bill/116th-congress/house-bill/6677? q=%7B%22search%22%3A%5B%22Privacy+protection%22%5D%7D&s=2&r=12.
[54] 冉连,张曦. 地方政府数据开放中的数据安全政策研究——基于全国33个地级市政策文本的内容分析[J/OL]. [2020-11-23]. http://kns. cnki. net/kcms/detail/61. 1167. G3. 20200811. 1014. 002. html.
[55] President memo: Freedom of information act[EB/OL]. [2020-11-16]. https://www. justice. gov/sites/default/files/oip/legacy/

2014/07/23/presidential-foia. pdf.
[56] Open data policy – Managing Information as an Asset[EB/OL]. [2020 – 06 – 26]. https://project-open-data. cio. gov/policy-memo/.
[57] Office of management and budget[EB/OL]. [2020 – 11 – 16]. https://www. white house. gov/omb/memoranda_m03-22.
[58] Organization, mission and functions manual: Office of information policy[EB/OL]. [2020 – 11 – 17]. https://www. justice. gov/jmd/organization-mission-and-functions-manual-office-information-policy.
[59] Chief information officers council [EB/OL]. [2020 – 06 – 28]. http://s3. amazonaws. com/sitesusa/Wp-content/uploads/sites/1151/2016/10/Standardized_Digital_Privacy_Controls. pdf.
[60] Federal privacy council [EB/OL]. [2020 – 11 – 17]. https://www. fpc. gov.
[61] National technical information service [EB/OL]. [2020 – 11 – 18]. https://www. ntis. gov/privacy/index. html.
[62] General services administration[EB/OL]. [2020 – 11 – 18]. https://www. gsa. gov/ reference/gsa-privacy-program.
[63] Federal data strategy [EB/OL]. [2020 – 11 – 18]. https://strategy. data. gov/background/.
[64] Personally identifiable information[EB/OL]. [2020 – 11 – 18]. https://www. investopedia. com/terms/p/personally-identifiable-information-pii. asp.
[65] Chief information officers council [EB/OL]. [2020 – 11 – 18]. https://www. cio. gov/policies-and-priorities/#subject = * &role = . privacy-filter&status = * .
[66] Networking and information technology research and development [EB/OL]. [2020 – 11 – 19]. https://www. nitrd. gov/about/index. aspx.
[67] Networking and information technology research and development [EB/OL]. [2020 – 11 – 19]. https://www. nitrd. gov/cybersecurity/nprsrfi102014/BigData-SP. pdf.
[68] Chief information officers council[EB/OL]. [2020 – 11 – 19]. http://s3. amazonaws. com/sitesusa/wp-content/uploads/sites/1151/2016/10/DHS-Privacy-Office-Guide_June-2010. pdf.
[69] Department of homeland security [EB/OL]. [2020 – 11 – 20]. https://www. dhs. gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007. pdf.
[70] Privacy impact assessment(PIA) guide [EB/OL]. [2020 – 11 – 21]. https://www. sec. gov/about/privacy/piaguide. pdf.
[71] 罗静怡. 政府部门计算机网络安全中数据加密技术的运用研究[J]. 通讯世界,2018(04):46 – 47.
[72] 丁红发,孟秋晴,王祥等. 面向数据生命周期的政府数据开放的数据安全与隐私保护对策分析[J]. 情报杂志,2019,38(7):151 – 159.
[73] 李凤华,李晖,贾焰等. 隐私计算研究范畴及发展趋势[J]. 通信学报,2016,37(4):1 – 11.

作者贡献说明:
储节旺:设计选题与论文修改指导;
丁辉:论文撰写与修改。

Personal Privacy Protection Policy of American Government's Open Data and Its Enlightenment to China
——Content Analysis Based on 52 Policy Texts

Chu Jiewang Ding Hui
Management School of Anhui University, Hefei 230601

Abstract: **[Purpose/significance]** Personal privacy protection is a key link in the process of government open data. By combing the personal privacy protection policies in the practice of American government open data, this paper provides some reference for the personal privacy protection in China's open government data. **[Method/process]** Through the collection of policy texts related to open data of the U. S. government, using NVivo text analysis tool, the content coding analysis of policy texts is carried out, and combing the U. S. government open data privacy protection framework, so as to obtain beneficial enlightenment and reference. **[Result/conclusion]** In order to give full play to the era value of government data opening, we should construct the personal privacy protection system from five dimensions: giving full play to the function of multiple subjects, building privacy protection evaluation system, privacy data utilization and governance, building privacy calculation model and legal protection.

Keywords: government open data policy text personal privacy protection America government open platform